EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S305	157	726/8.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 11:59
S306	1377	326/39.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:01
S307	1154	713/189.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:02
S308	682	713/170.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:02
S309	606	713/165.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:03
S310	1688	713/193.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:03
S311	459	713/194.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:03
S312	3606	(FPGA) and (hash or MAC)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:05
S313	3861	(FPGA) and (hash$4 or MAC or message adj2 authenticat$4 adj4 code)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:07

EAST Search History

S314	19657	symmetric near3 key or secret near3 key	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:06
S315	364	S313 and S314	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:06
S316	38858	(FPGA) or (field adj2 program$5 adj3 gate adj4 array)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:07
S317	4269	S316 and (hash$4 or MAC or message adj2 authenticat$4 adj4 code)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:07
S318	382	S316 and (hash$4 or MAC or message adj2 authenticat$4 adj4 code) and S314	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/02/28 12:08
S319	1	(FPGA and chip and nonvolatile and (secret or symmetric) and key and MAC and external).CLM.	US-PGPUB; USPAT	OR	ON	2007/02/28 12:09

PORTAL

USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

FPGA and secret key SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used FPGA and secret key

Found 5,498 of 198,146

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

☐ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200

Best 200 shown

Result page: **1** 2 3 4 5 6 7 8 9 10 next

Relevance scale

1 Design and Implementation of a Secret Key Steganographic Micro-Architecture Employing FPGA

Hala Farouk, Magdy Saeb

February 2004 **Proceedings of the conference on Design, automation and test in Europe - Volume 3 DATE '04**

Publisher: IEEE Computer Society

Full text available: pdf(280.16 KB) Additional Information: full citation, abstract, index terms

In the well-known "prisoners' problem", a representative example of steganography, two persons attempt to communicate covertly without alerting the warden. One approach to achieve this task is to embed the message in an innocent-looking cover-media. In our model, the message contents are scattered in the cover in a certain way that is based on a secret key known only to the sender and receiver. Therefore, even if the warden discovers theexistence of the message, he will not be able to recover it ...

Keywords: Steganography, data hiding, FPGA, architecture, covert communications, subliminal channel

2 (Special session) presentation + poster disscussion: university design contest: Design and implementation of a secret key steganographic micro-architecture employing FPGA

Hala A. Farouk, Magdy Saeb

January 2004 **Proceedings of the 2004 conference on Asia South Pacific design automation: electronic design and solution fair ASP-DAC '04 , Proceedings of the 2004 conference on Asia South Pacific design automation: electronic design and solution fair ASP-DAC '04**

Publisher: IEEE Press

Full text available: pdf(307.02 KB) Publisher Site Additional Information: full citation, abstract

In the well-known "prisoners' problem", a representative example of steganography, two persons attempt to communicate covertly without alerting the warden. One approach to achieve this task is to embed the message contents are scattered in the cover in a certain way that is based on a secret key known only to the sender and receiver. Therefore, even if the warden discovers the existence of the message, he will not be able to recover it. In other words a covert or subliminal communication channel ...

3 Fast implementations of secret-key block ciphers using mixed inner- and outer-round pipelining

Pawel Chodowiec, Po Khuon, Kris Gaj

February 2001 **Proceedings of the 2001 ACM/SIGDA ninth international symposium on Field programmable gate arrays FPGA '01**

Publisher: ACM Press

Full text available: pdf(691.29 KB) Additional Information: full citation, abstract, references, citings, index terms

The new design methodology for secret-key block ciphers, based on introducing an optimum number of pipeline stages inside of a cipher round is presented and evaluated. This methodology is applied to five well-known modern ciphers, Triple DES, Rijndael, RC6, Serpent, and Twofish, with the goal to first obtain the architecture with the optimum throughput to area ratio, and then the architecture with the highest possible throughput. All ciphers are modeled in VHDL, and implemented using Xilinx ...

Keywords: AES, fast architectures, pipelining, secret-key ciphers

4 Cellular and Cryptographic Applications: Cryptographic rights management of FPGA intellectual property cores
Tom Kean
February 2002 **Proceedings of the 2002 ACM/SIGDA tenth international symposium on Field-programmable gate arrays FPGA '02**
Publisher: ACM Press
Full text available: pdf(171.79 KB) Additional Information: full citation, abstract, references, index terms

As the capacity of FPGA's increases to millions of equivalent gates the use of Intellectual Property (IP) cores becomes increasingly important to control design complexity. FPGA's are becoming platforms for integrating a system solution from components supplied by independent vendors in the same way as printed circuit boards provided a platform for earlier generations of designers. However, the current commercial model for IP cores involves large up-front license fees reminiscent of ASIC NRE cha ...

Keywords: FPGA, cryptography, intellectual property, rights management

5 Security on FPGAs: State-of-the-art implementations and attacks
Thomas Wollinger, Jorge Guajardo, Christof Paar
August 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 3
Publisher: ACM Press
Full text available: pdf(296.79 KB) Additional Information: full citation, abstract, references, index terms

In the last decade, it has become apparent that embedded systems are integral parts of our every day lives. The wireless nature of many embedded applications as well as their omnipresence has made the need for security and privacy preserving mechanisms particularly important. Thus, as field programmable gate arrays (FPGAs) become integral parts of embedded systems, it is imperative to consider their security as a whole. This contribution provides a state-of-the-art description of security issues ...

Keywords: Cryptography, FPGA, attacks, cryptographic applications, reconfigurable hardware, reverse engineering, security

6 Reconfigurable hardware solutions for the digital rights management of digital cinema
G. Rouvroy, F.-X. Standaert, F. Lefèbvre, J.-J. Quisquater, B. Macq, J.-D. Legat
October 2004 **Proceedings of the 4th ACM workshop on Digital rights management DRM '04**
Publisher: ACM Press
Full text available: pdf(440.86 KB) Additional Information: full citation, abstract, references, index terms

This paper presents a hardware implementation of a decoder for Digital Cinema images. This decoder enables us to deal with image size of 2K with 24 frames per second and 36 bits per pixels. It is the first implementation known nowadays that perfectly fits in one single Virtex-II® FPGA and includes AES decryption, JPEG 2000 decompression and fingerprinting blocks. This hardware offers therefore high-quality image processing as well as robust security.

Keywords: AES, DRM, FPGA, JPEG 2000, digital cinema, watermarking

7 An Improved FPGA Implementation of the Modified Hybrid Hiding Encryption Algorithm (MHHEA) for Data Communication Security
Hala A. Farouk, Magdy Saeb

PORTAL

USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

FPGA and MAC

SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used FPGA and MAC

Found 5,944 of 198,146

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200

Result page: 1 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 Computation algorithms for FPGA: Floating-point sparse matrix-vector multiply for FPGAs

Michael deLorimier, André DeHon

February 2005 **Proceedings of the 2005 ACM/SIGDA 13th international symposium on Field-programmable gate arrays FPGA '05**

Publisher: ACM Press

Full text available: pdf(344.21 KB) Additional Information: full citation, abstract, references, citings, index terms

Large, high density FPGAs with high local distributed memory bandwidth surpass the peak floating-point performance of high-end, general-purpose processors. Microprocessors do not deliver near their peak floating-point performance on efficient algorithms that use the Sparse Matrix-Vector Multiply (SMVM) kernel. In fact, it is not uncommon for microprocessors to yield only 10--20% of their peak floating-point performance when computing SMVM. We develop and analyze a scalable SMVM implementation on ...

Keywords: FPGA, compressed sparse row, floating point, reconfigurable architecture, sparse matrix

2 FPGA-based sonar processing

Paul Graham, Brent Nelson

March 1998 **Proceedings of the 1998 ACM/SIGDA sixth international symposium on Field programmable gate arrays FPGA '98**

Publisher: ACM Press

Full text available: pdf(1.21 MB) Additional Information: full citation, abstract, references, citings, index terms

This paper presents the application of time-delay sonar beamforming and discusses a multi-board FPGA system for performing several variations of this beamforming method in real-time for realistic sonar arrays. Additionally, we show that our proposed FPGA system has a six to twelve times performance advantage over an equivalent system created using currently available, high-performance DSPs designed for multiprocessing systems. This performance advantage is due to the simplicity of the core ...

3 Computation algorithms for FPGA: 64-bit floating-point FPGA matrix multiplication

Yong Dou, S. Vassiliadis, G. K. Kuzmanov, G. N. Gaydadjiev

February 2005 **Proceedings of the 2005 ACM/SIGDA 13th international symposium on Field-programmable gate arrays FPGA '05**

Publisher: ACM Press

Full text available: pdf(532.78 KB) Additional Information: full citation, abstract, references, index terms

We introduce a 64-bit ANSI/IEEE Std 754-1985 floating point design of a hardware matrix multiplier optimized for FPGA implementations. A general block matrix multiplication algorithm, applicable for an arbitrary matrix size is proposed. The algorithm potentially enables optimum performance by exploiting the data locality and reusability incurred by the general matrix multiplication scheme and considering the limitations of the I/O bandwidth and the local storage volume. We implement a scalable l ...

Keywords: FPGA, floating-point, matrix multiplication

4 Novel FPGA applications: CUSP: a modular framework for high speed network applications on FPGAs

Graham Schelle, Dirk Grunwald

February 2005 **Proceedings of the 2005 ACM/SIGDA 13th international symposium on Field-programmable gate arrays FPGA '05**

Publisher: ACM Press

Full text available: pdf(547.03 KB) Additional Information: full citation, abstract, references, citings, index terms

For several years now, modern FPGAs have included onchip network related hard cores. These cores include Xilinx's RocketIO and Altera's RapidIO serial transceivers. However, to use these cores in a complete networking application may be a daunting task to a non-networking expert. In addition to the complicated use of these components, the high performance needs of modern networking applications require designs that are optimized for low latency and a moderately high clock rate. Therefore to meet ...

Keywords: networking, parallelism, reconfigurable hardware, speculation

5 Security: The shunt: an FPGA-based accelerator for network intrusion prevention

Nicholas Weaver, Vern Paxson, Jose M. Gonzalez

February 2007 **Proceedings of the 2007 ACM/SIGDA 15th international symposium on Field programmable gate arrays FPGA '07**

Publisher: ACM Press

Full text available: pdf(240.27 KB) Additional Information: full citation, abstract, references, index terms

The sophistication and complexity of analysis performed by today's network intrusion prevention systems (IPSs) benefits greatly from implementation using general-purpose CPUs. Yet the performance of such CPUs increasingly lags behind that necessary to process today's high-rate traffic streams. A key observation, however, is that much of the traffic comprising a high-volume stream can, after some initial analysis, be qualified as "likely uninteresting." To this end, we have developed an in-line, ...

Keywords: FPGA, NIC, hardware acceleration, intrusion detection

6 Parameterized MAC unit implementation

Ming-Chih Chen, Ing-Jer Huang, Chung-Ho Chen

January 2001 **Proceedings of the 2001 conference on Asia South Pacific design automation ASP-DAC '01**

Publisher: ACM Press

Full text available: pdf(79.23 KB) Additional Information: full citation, abstract, references, index terms

Ethernet communication devices, such as adapter, hub, bridge and switch, all follow IEEE 802.3 standard protocol. We have designed and implemented an integrated 10/100 Mbps Ethernet MAC (Medium Access Control) mechanism. The MAC unit is used to handle receive/transmit processes of network packet stream. To meet the requirement of different communication devices, we design an automatic MAC unit generator. Users can select the desired number of MAC units through parametric environment setup. ...

7 Effective Co-Verification of IEEE 802.11a MAC/PHY Combining Emulation and Simulation Technology

IL-Gu Lee, Seung-Beom Lee, Sin-Chong Park

April 2005 **Proceedings of the 38th annual Symposium on Simulation ANSS '05**

Publisher: IEEE Computer Society

Full text available: pdf(358.72 KB) Additional Information: full citation, abstract, index terms

This work presents a system architecture and effective co-verification methodologies for the IEEE 802.11a Medium Access Control (MAC) layer/Physical (PHY) layer implementation. The architecture modeling includes hardware/software partitioning of a total system based on timing measurements from the C/C++ and Verilog design, and analysis of real-time requirements specified in the standard. The system is built on an evaluation platform that contains a Xilinx Virtex-II FPGA and an Altera Excalibur A ...

8 Design Space Exploration for a Wireless Protocol on a Reconfigurable Platform

[File 2] **INSPEC** 1898-2007/Feb W3
(c) 2007 Institution of Electrical Engineers. All rights reserved.

[File 6] **NTIS** 1964-2007/Feb W4
(c) 2007 NTIS, Intl Cpyrght All Rights Res. All rights reserved.

[File 8] **Ei Compendex(R)** 1884-2007/Feb W3
(c) 2007 Elsevier Eng. Info. Inc. All rights reserved.

[File 34] **SciSearch(R) Cited Ref Sci** 1990-2007/Feb W3
(c) 2007 The Thomson Corp. All rights reserved.

[File 434] **SciSearch(R) Cited Ref Sci** 1974-1989/Dec
(c) 2006 The Thomson Corp. All rights reserved.

[File 35] **Dissertation Abs Online** 1861-2007/Feb
(c) 2007 ProQuest Info&Learning. All rights reserved.

[File 62] **SPIN(R)** 1975-2007/Feb W2
(c) 2007 American Institute of Physics. All rights reserved.

[File 65] **Inside Conferences** 1993-2007/Feb 28
(c) 2007 BLDSC all rts. reserv. All rights reserved.

[File 99] **Wilson Appl. Sci & Tech Abs** 1983-2007/Feb
(c) 2007 The HW Wilson Co. All rights reserved.

[File 144] **Pascal** 1973-2007/Feb W3
(c) 2007 INIST/CNRS. All rights reserved.

[File 266] **FEDRIP** 2007/Jan
Comp & dist by NTIS, Intl Copyright All Rights Res. All rights reserved.

[File 275] **Gale Group Computer DB(TM)** 1983-2007/Feb 27
(c) 2007 The Gale Group. All rights reserved.

[File 621] **Gale Group New Prod.Annou.(R)** 1985-2007/Feb 19
(c) 2007 The Gale Group. All rights reserved.

[File 674] **Computer News Fulltext** 1989-2006/Sep W1
(c) 2006 IDG Communications. All rights reserved.
**File 674: File 674 is closed (no longer updates).*

```
?  s FPGA or field (2n) program? (2n) gate (2n) array?
Processing
        38937   FPGA
      4737778   FIELD
```

```
         4581316   PROGRAM?
          328464   GATE
          970443   ARRAY?
           34329   FIELD(2N)PROGRAM?(2N)GATE(2N)ARRAY?
S1         47741   S FPGA OR FIELD (2N) PROGRAM? (2N) GATE (2N) ARRAY?

?  s secret (2n) key? or symmetric (2n) key?
           55484   SECRET
         1948952   KEY?
            5774   SECRET(2N)KEY?
          324275   SYMMETRIC
         1948952   KEY?
            1392   SYMMETRIC(2N)KEY?
S2          7001   S SECRET (2N) KEY? OR SYMMETRIC (2N) KEY?

?  s MAC or message (2n) authenticat? (2n) code?
          146779   MAC
          278410   MESSAGE
           90221   AUTHENTICAT?
         1322898   CODE?
             830   MESSAGE(2N)AUTHENTICAT?(2N)CODE?
S3        147195   S MAC OR MESSAGE (2N) AUTHENTICAT? (2N) CODE?

?  s s1 and s2 and s3
           47741   S1
            7001   S2
          147195   S3
S4             2   S S1 AND S2 AND S3
```